FIG. 1

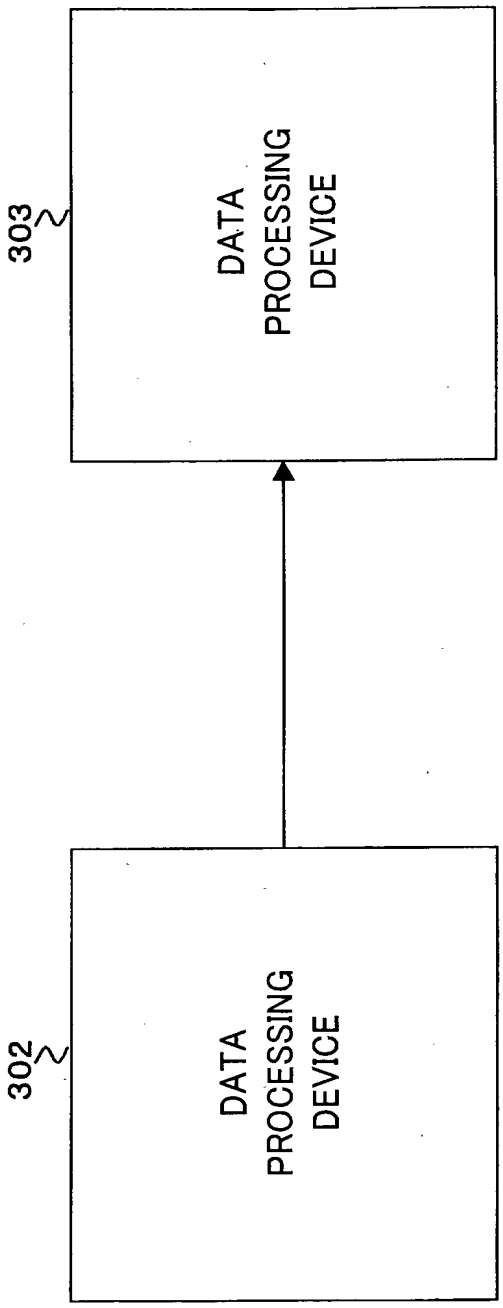


FIG. 2

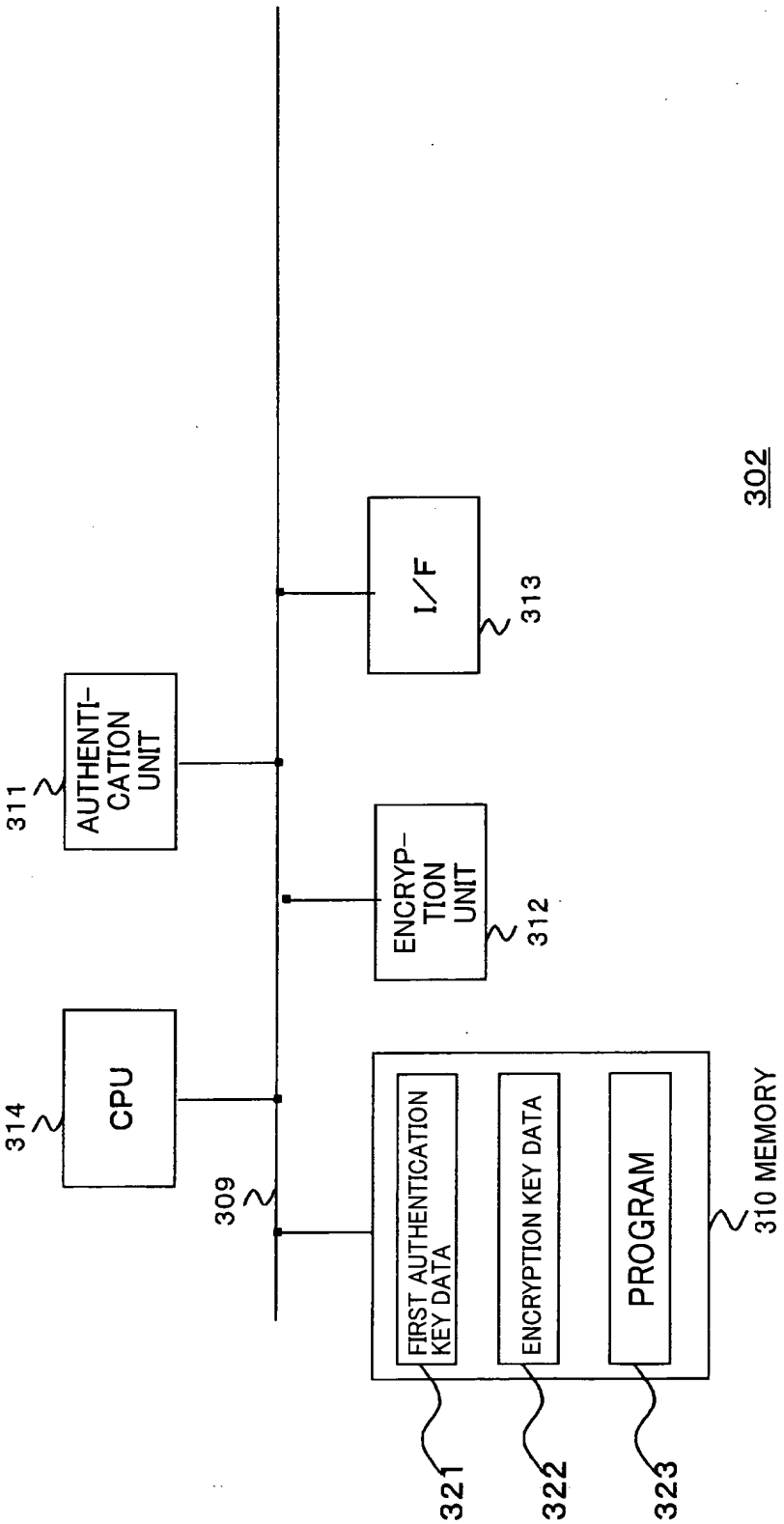

302
I/F
313
AUTHENTI-
CATION
UNIT
311
ENCRYP-
TION
UNIT
312
CPU
314
309
FIRST AUTHENTICATION
KEY DATA
ENCRYPTION KEY DATA
PROGRAM
310 MEMORY
321
322
323

FIG. 3

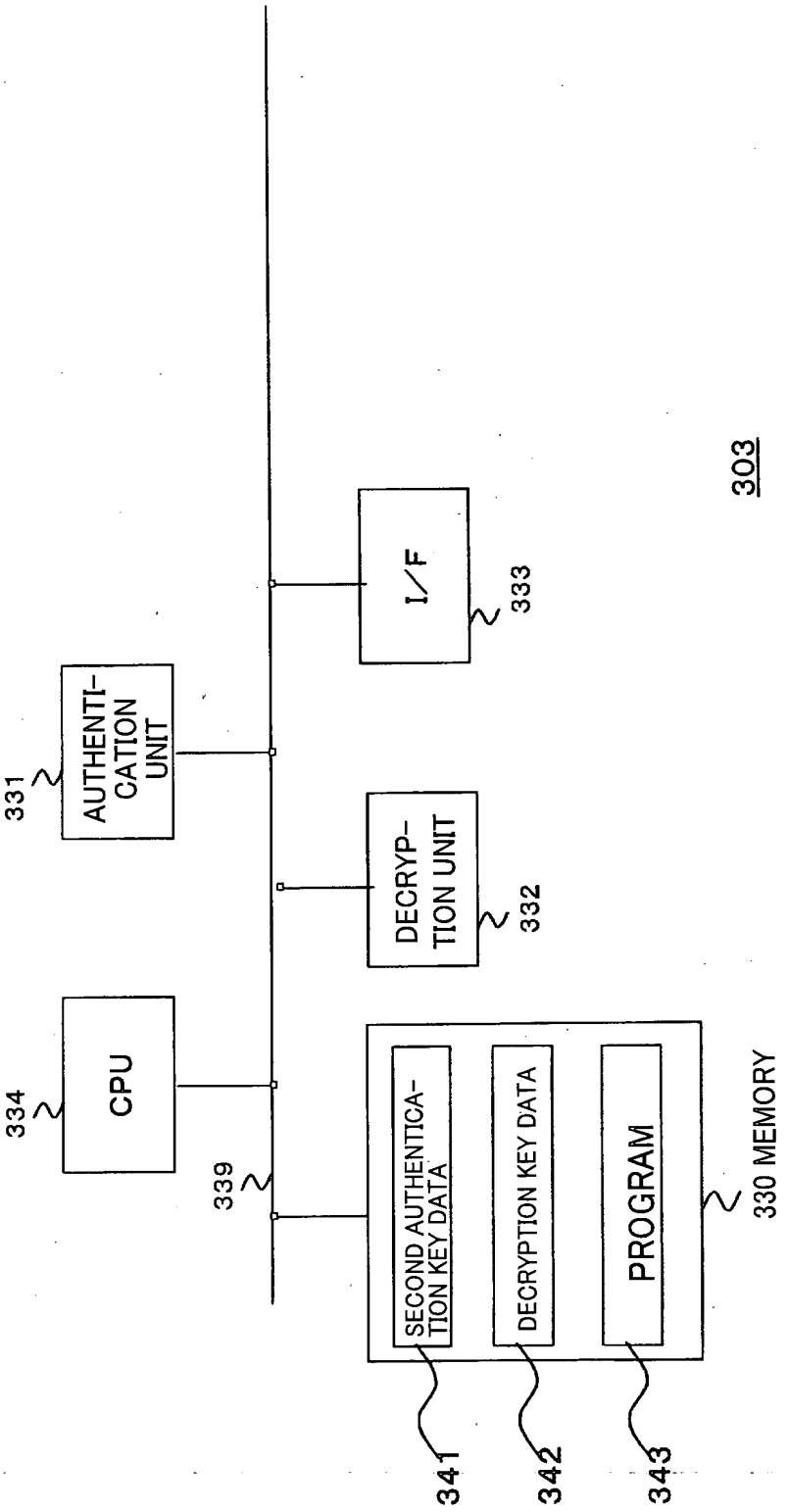

303
I/F
333
AUTHENTI-
CATION
UNIT
331
DECRYP-
TION UNIT
332
CPU
334
339
SECOND AUTHENTICA-
TION KEY DATA
DECRYPTION KEY DATA
PROGRAM
330 MEMORY
341
342
343

FIG. 4

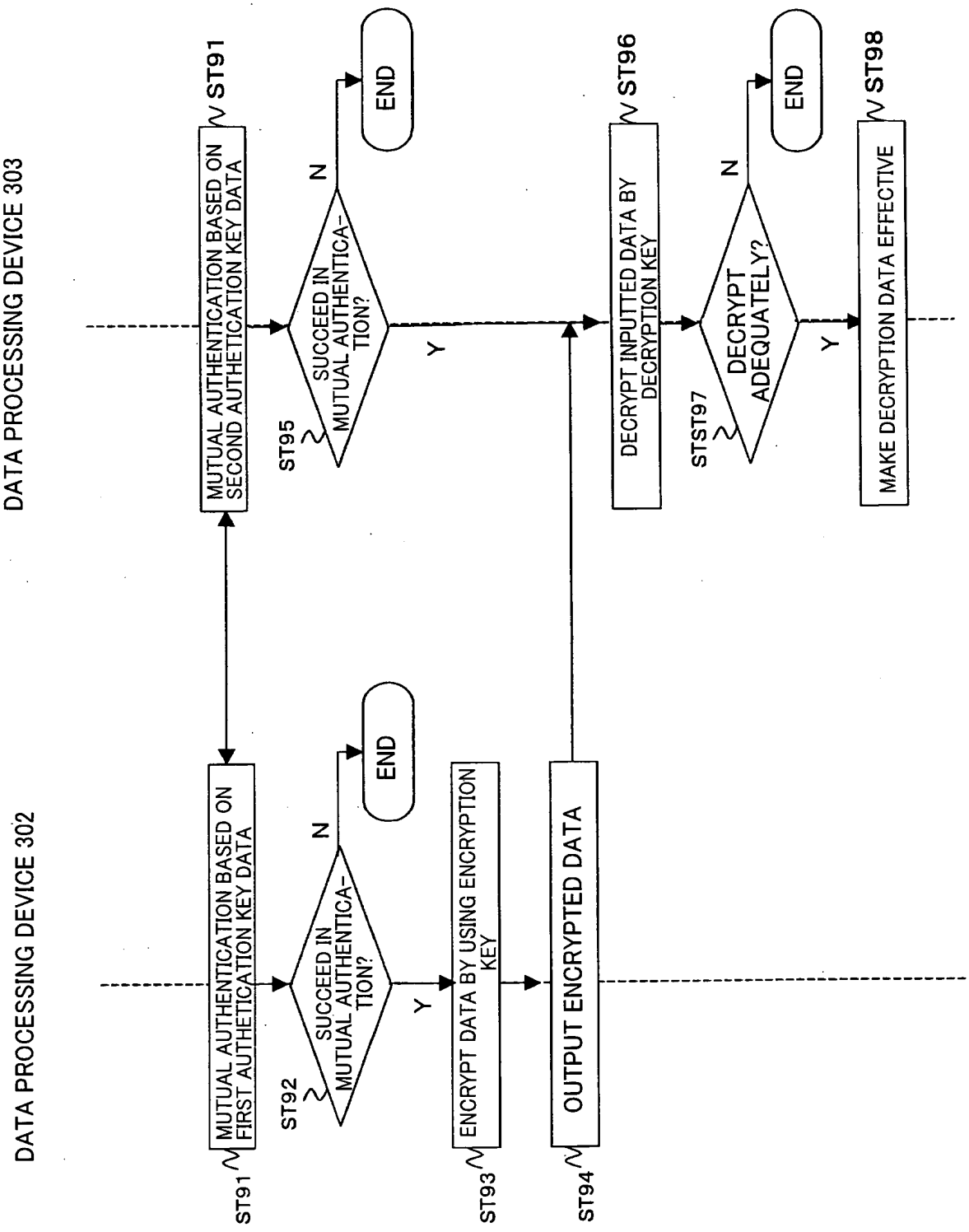

DATA PROCESSING DEVICE 302
DATA PROCESSING DEVICE 303
MUTUAL AUTHENTICATION BASED ON FIRST AUTHETICATION KEY DATA
ST91
SUCCEED IN MUTUAL AUTHENTICATION?
ST92
N
END
Y
ENCRYPT DATA BY USING ENCRYPTION KEY
ST93
OUTPUT ENCRYPTED DATA
ST94
MUTUAL AUTHENTICATION BASED ON SECOND AUTHETICATION KEY DATA
ST91
SUCCEED IN MUTUAL AUTHENTICATION?
ST95
N
END
Y
DECRYPT INPUTTED DATA BY DECRYPTION KEY
ST96
DECRYPT ADEQUATELY?
STST97
N
END
Y
MAKE DECRYPTION DATA EFFECTIVE
ST98

FIG. 5

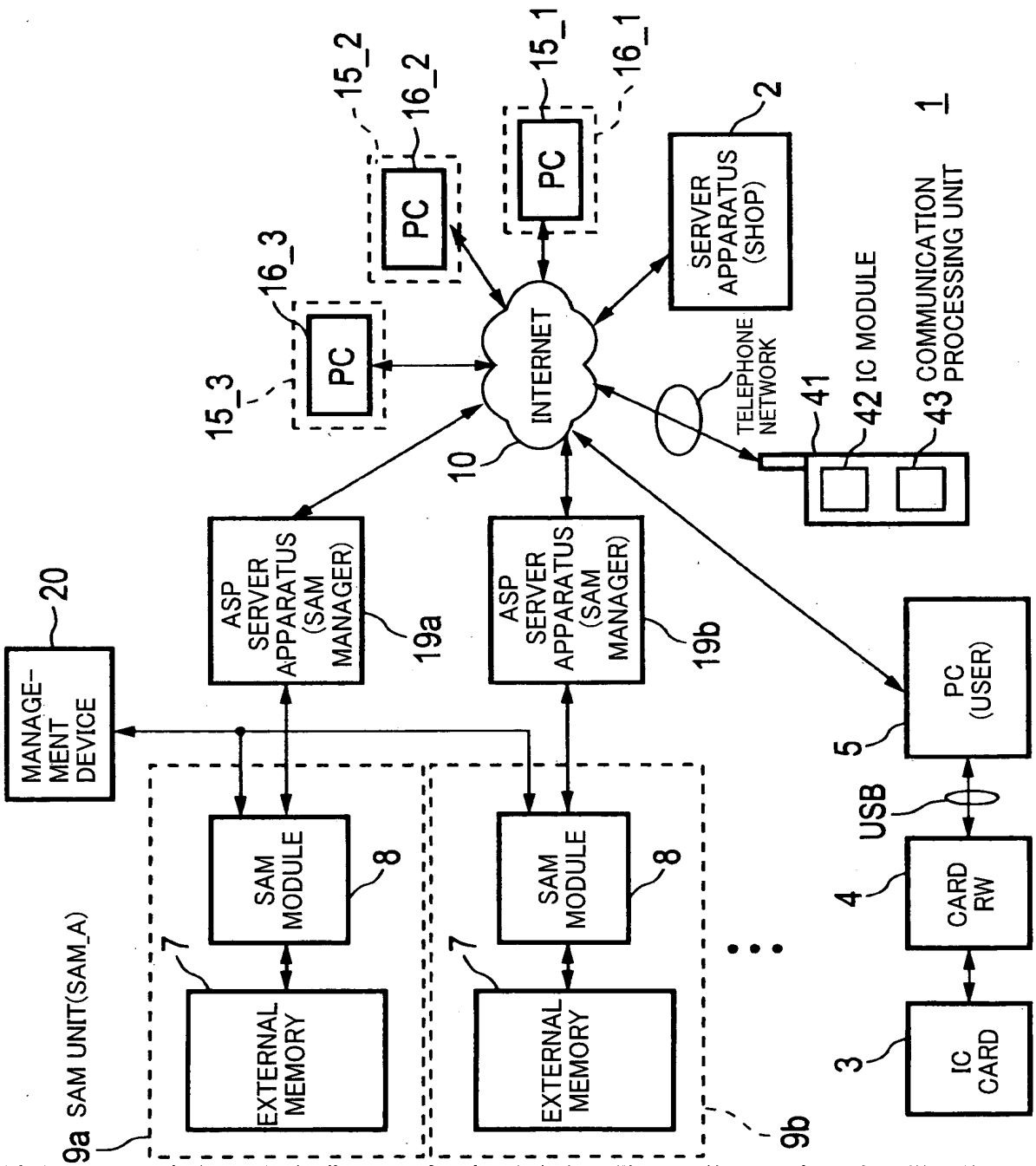

1
2
PC
15_1
16_1
15_2
16_2
15_3
16_3
SERVER APPARATUS (SHOP)
INTERNET
10
TELEPHONE NETWORK
41
42 IC MODULE
43 COMMUNICATION PROCESSING UNIT
20
MANAGE-MENT DEVICE
ASP SERVER APPARATUS (SAM MANAGER)
19a
19b
PC (USER)
5
USB
4
CARD RW
3
IC CARD
SAM MODULE
8
7
EXTERNAL MEMORY
9a SAM UNIT(SAM_A)
9b

FIG. 6

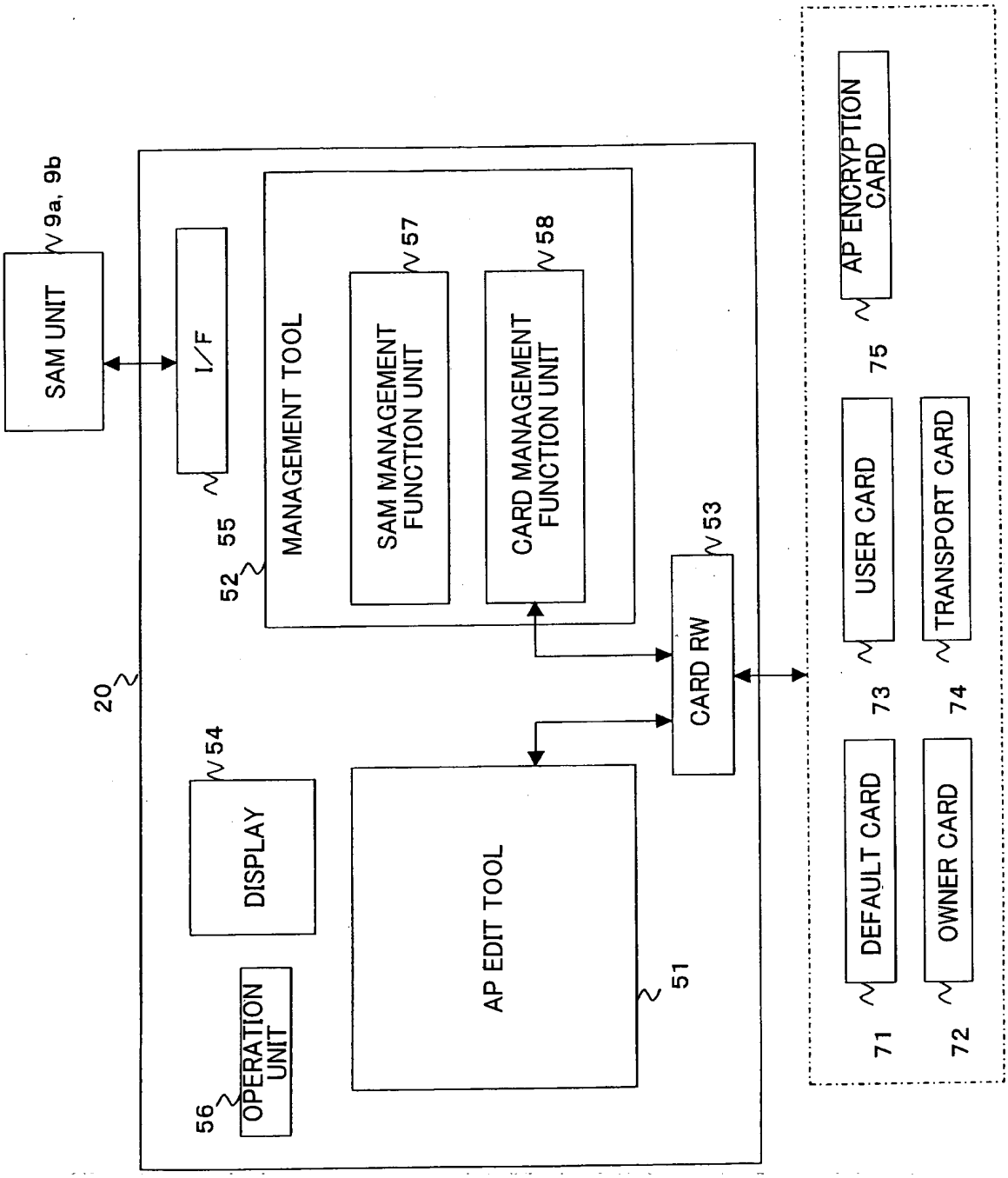

SAM UNIT
9a, 9b
I/F
55
MANAGEMENT TOOL
52
SAM MANAGEMENT FUNCTION UNIT
57
CARD MANAGEMENT FUNCTION UNIT
58
CARD RW
53
AP ENCRYPTION CARD
75
USER CARD
73
TRANSPORT CARD
74
DEFAULT CARD
71
OWNER CARD
72
20
DISPLAY
54
AP EDIT TOOL
51
OPERATION UNIT
56

FIG. 7

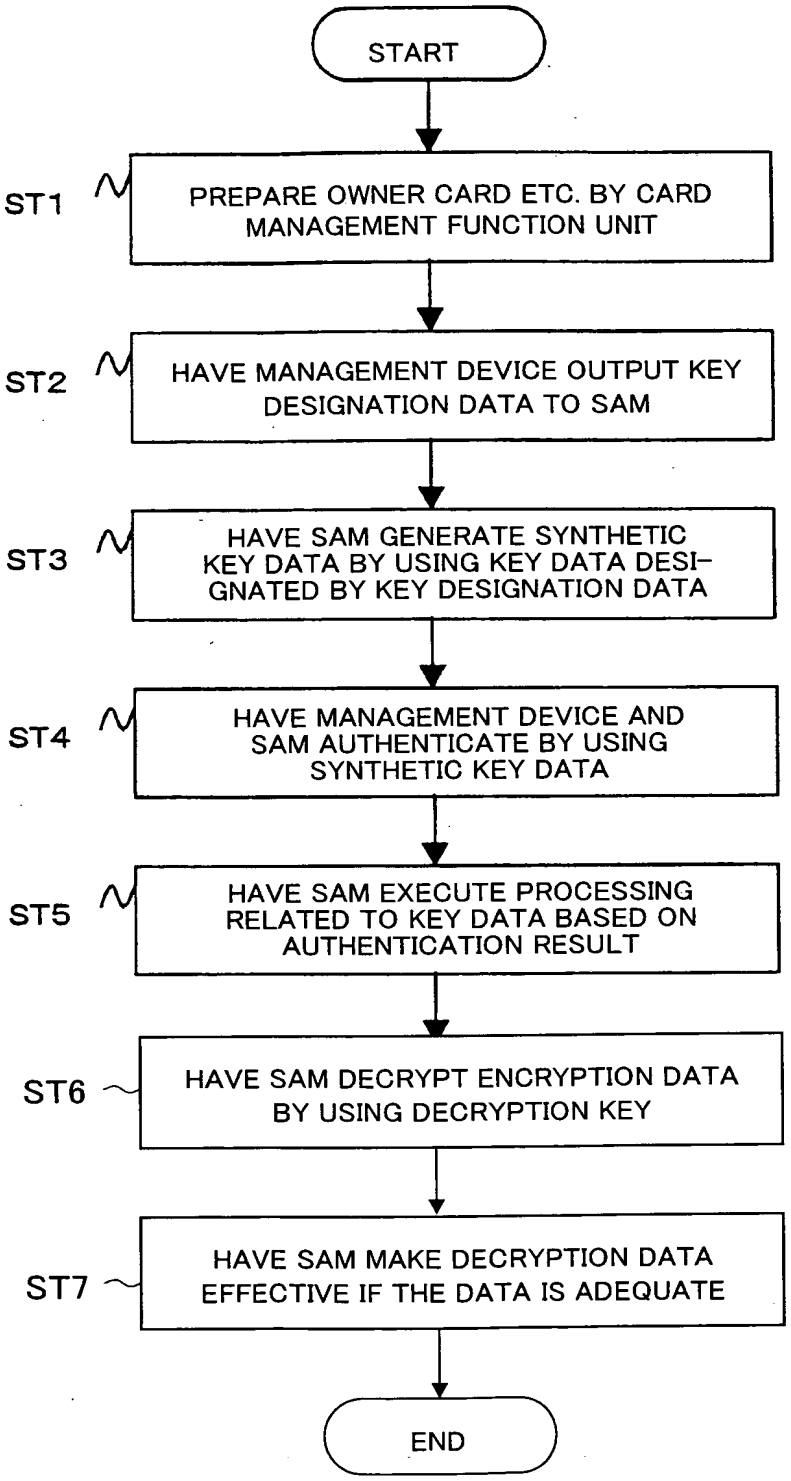

START
ST1
PREPARE OWNER CARD ETC. BY CARD MANAGEMENT FUNCTION UNIT
ST2
HAVE MANAGEMENT DEVICE OUTPUT KEY DESIGNATION DATA TO SAM
ST3
HAVE SAM GENERATE SYNTHETIC KEY DATA BY USING KEY DATA DESIGNATED BY KEY DESIGNATION DATA
ST4
HAVE MANAGEMENT DEVICE AND SAM AUTHENTICATE BY USING SYNTHETIC KEY DATA
ST5
HAVE SAM EXECUTE PROCESSING RELATED TO KEY DATA BASED ON AUTHENTICATION RESULT
ST6
HAVE SAM DECRYPT ENCRYPTION DATA BY USING DECRYPTION KEY
ST7
HAVE SAM MAKE DECRYPTION DATA EFFECTIVE IF THE DATA IS ADEQUATE
END

FIG. 8

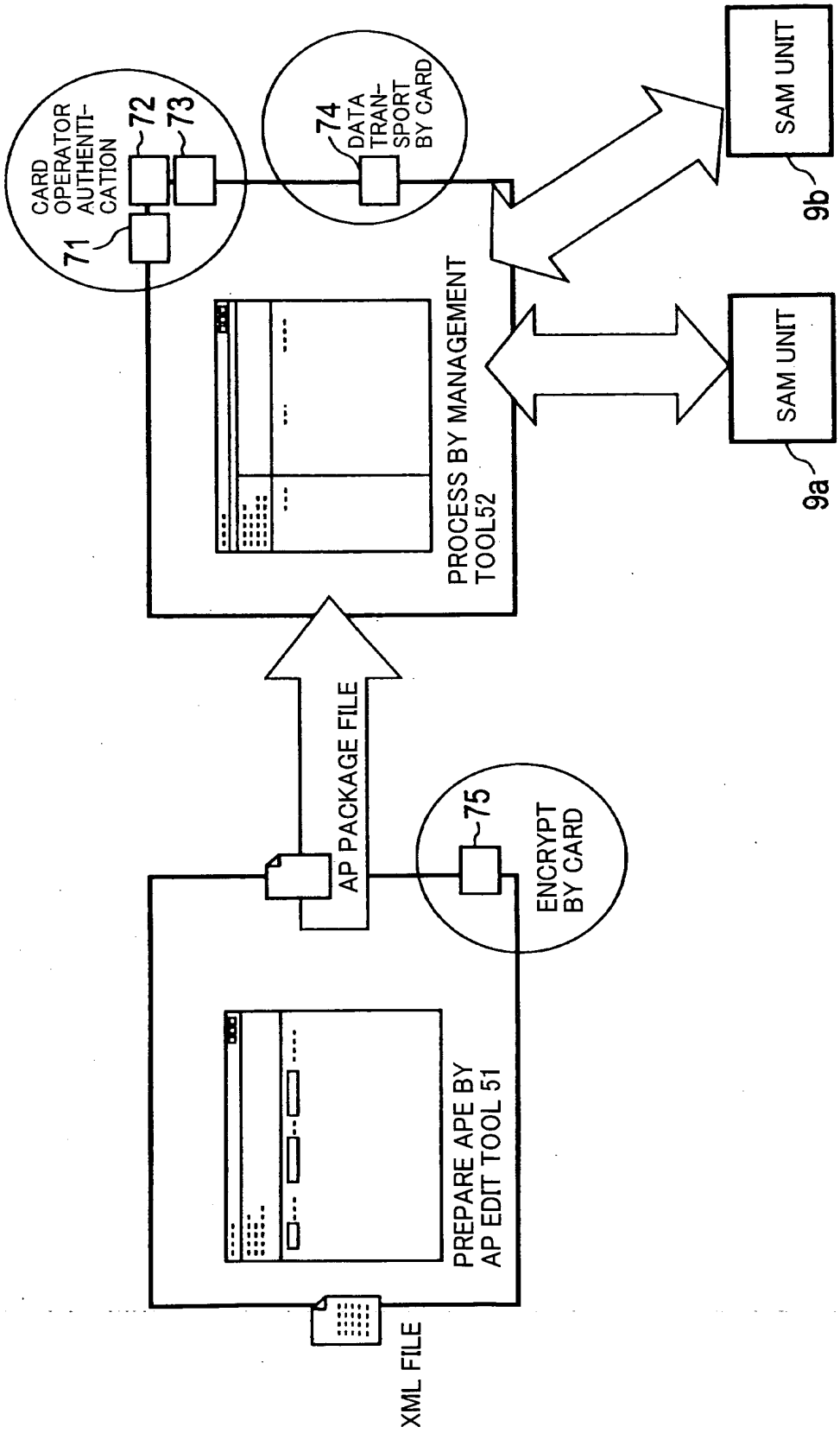

CARD OPERATOR AUTHENTI-CATION
71
72
73
74
DATA TRAN-SPORT BY CARD
SAM UNIT
9b
SAM UNIT
9a
PROCESS BY MANAGEMENT TOOL52
AP PACKAGE FILE
75
ENCRYPT BY CARD
PREPARE APE BY AP EDIT TOOL 51
XML FILE

FIG. 9

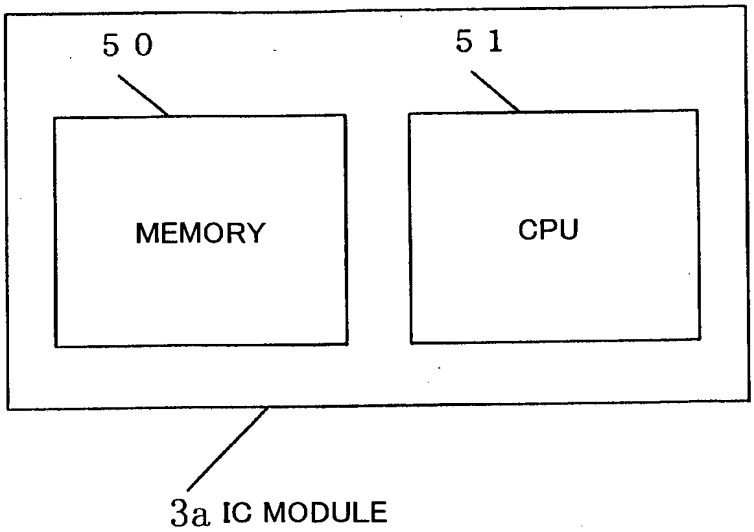

5 0
5 1
MEMORY
CPU
3a IC MODULE

FIG. 10

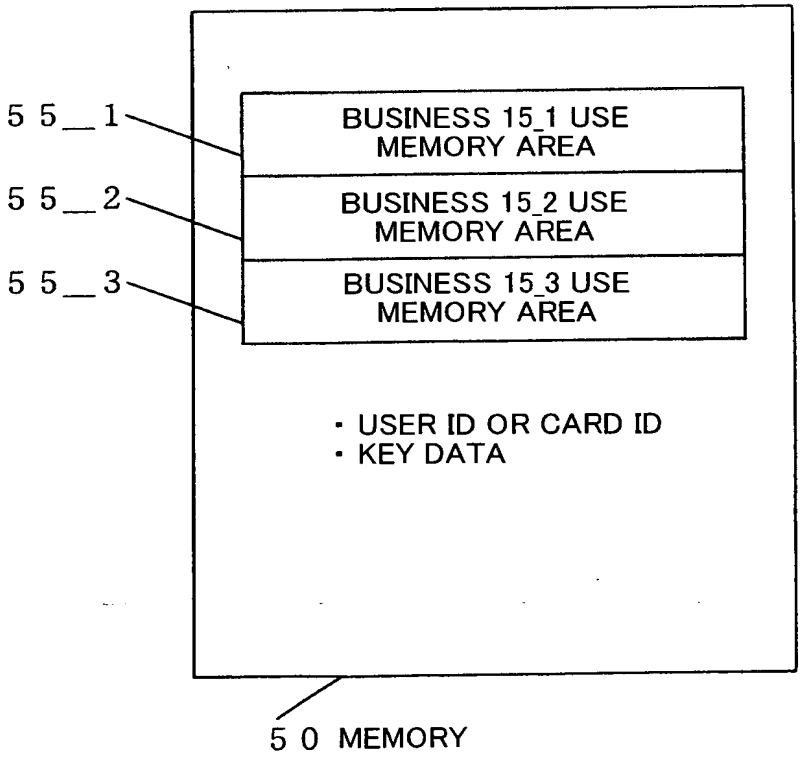

5 5__1
5 5__2
5 5__3
BUSINESS 15_1 USE MEMORY AREA
BUSINESS 15_2 USE MEMORY AREA
BUSINESS 15_3 USE MEMORY AREA
• USER ID OR CARD ID
• KEY DATA
5 0 MEMORY

FIG. 11

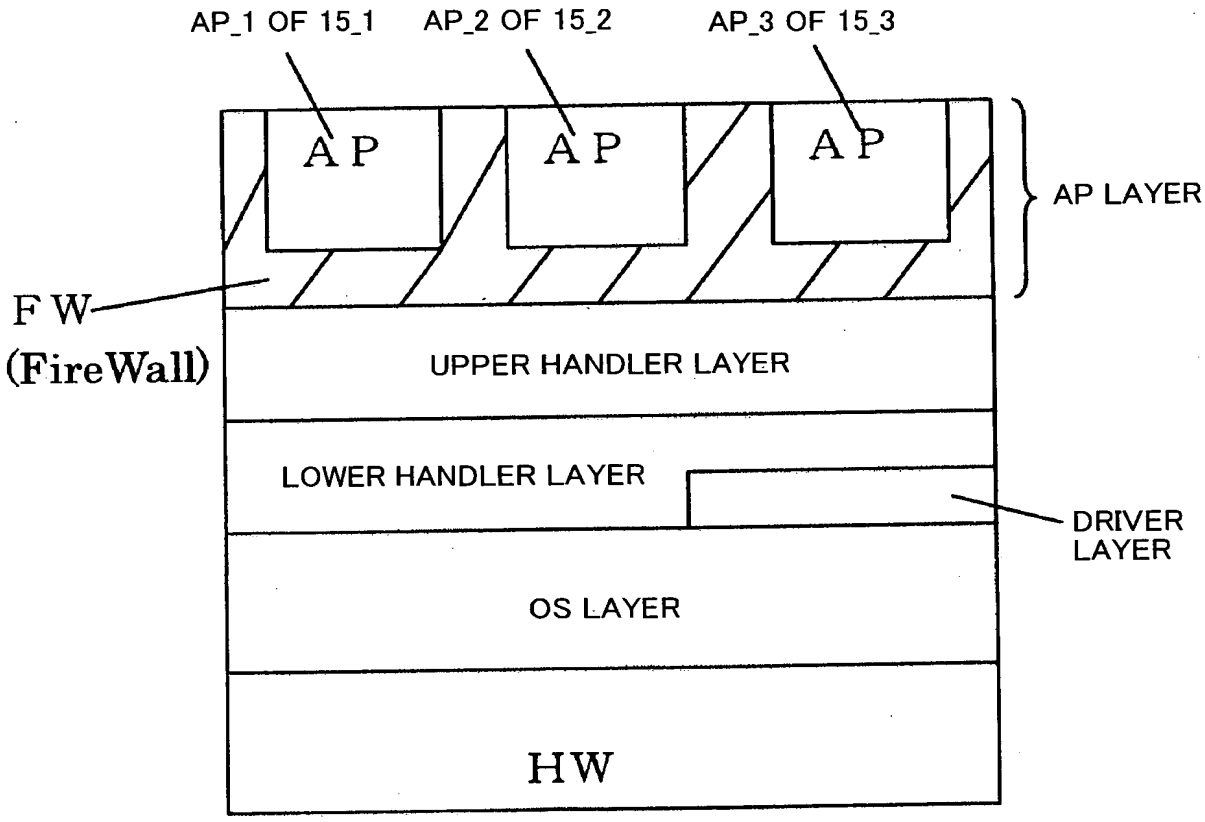

AP_1 OF 15_1
AP_2 OF 15_2
AP_3 OF 15_3
AP
AP
AP
AP LAYER
FW
(FireWall)
UPPER HANDLER LAYER
LOWER HANDLER LAYER
DRIVER LAYER
OS LAYER
HW

FIG. 12

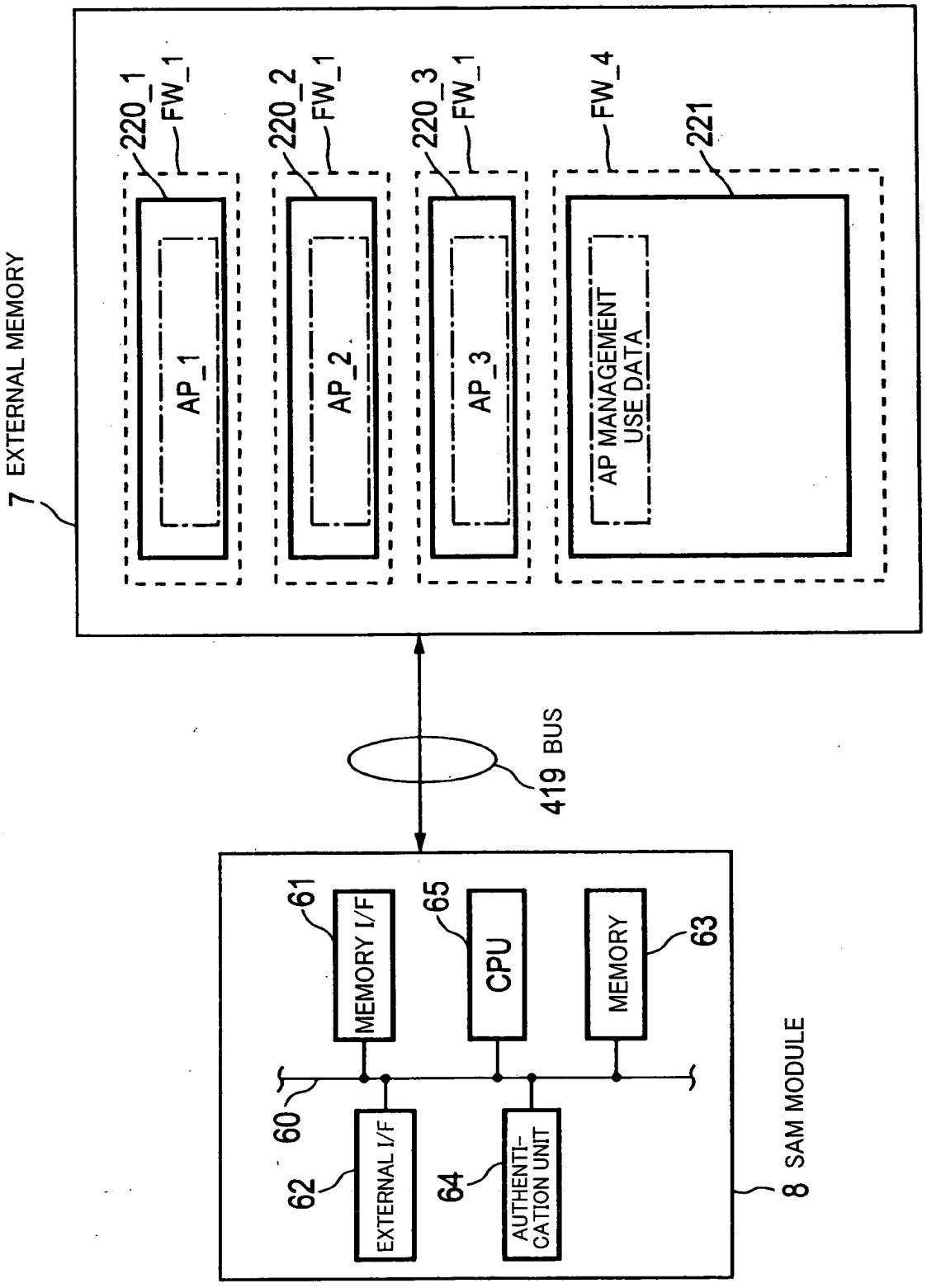

7 EXTERNAL MEMORY
220_1
FW_1
AP_1
220_2
FW_1
AP_2
220_3
FW_1
AP_3
FW_4
221
AP MANAGEMENT USE DATA
419 BUS
61
MEMORY I/F
65
CPU
63
MEMORY
60
62
EXTERNAL I/F
64
AUTHENTI-CATION UNIT
8 SAM MODULE

FIG. 13

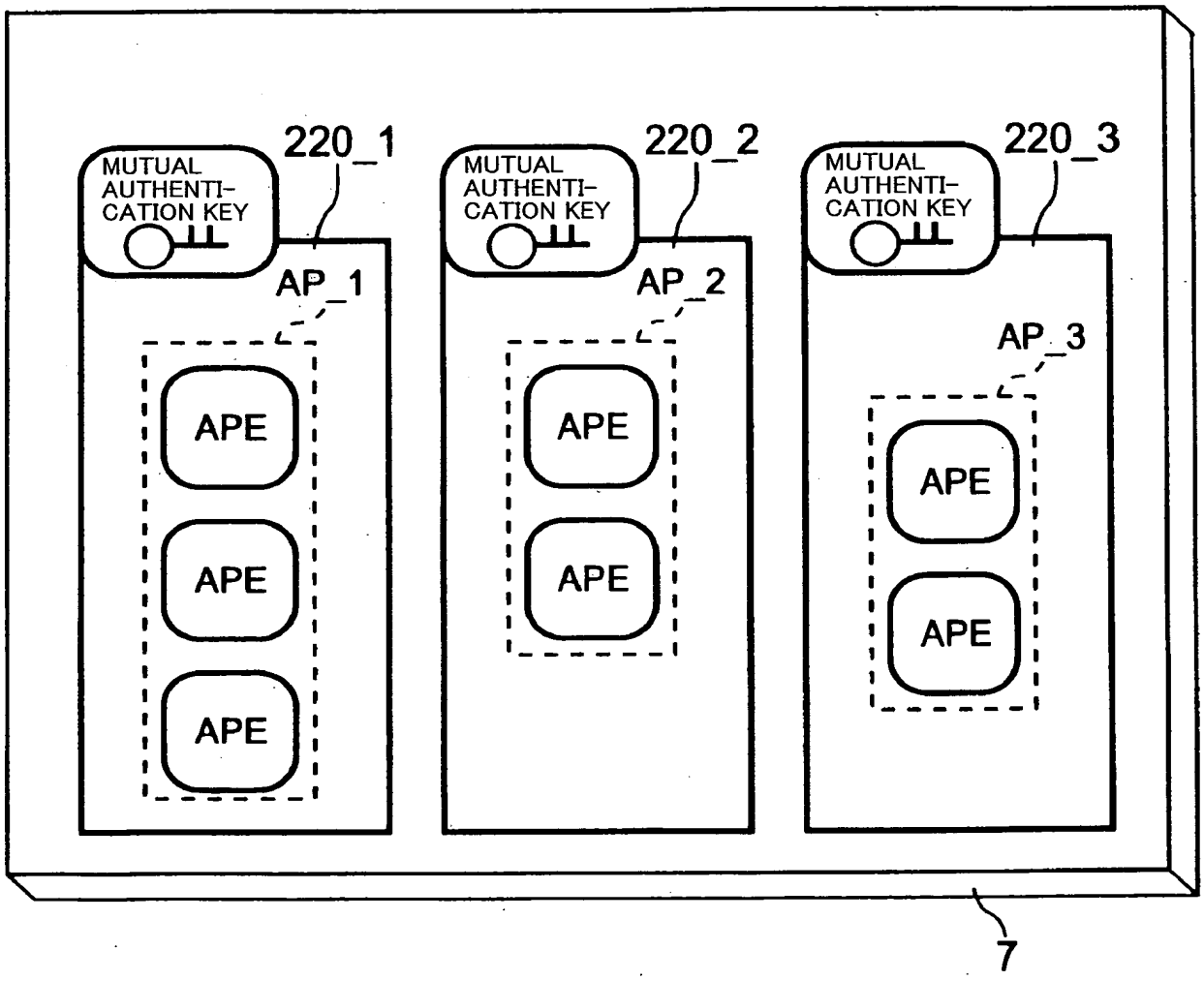

MUTUAL AUTHENTI-CATION KEY
220_1
AP_1
APE
APE
APE
MUTUAL AUTHENTI-CATION KEY
220_2
AP_2
APE
APE
MUTUAL AUTHENTI-CATION KEY
220_3
AP_3
APE
APE
7

FIG. 14

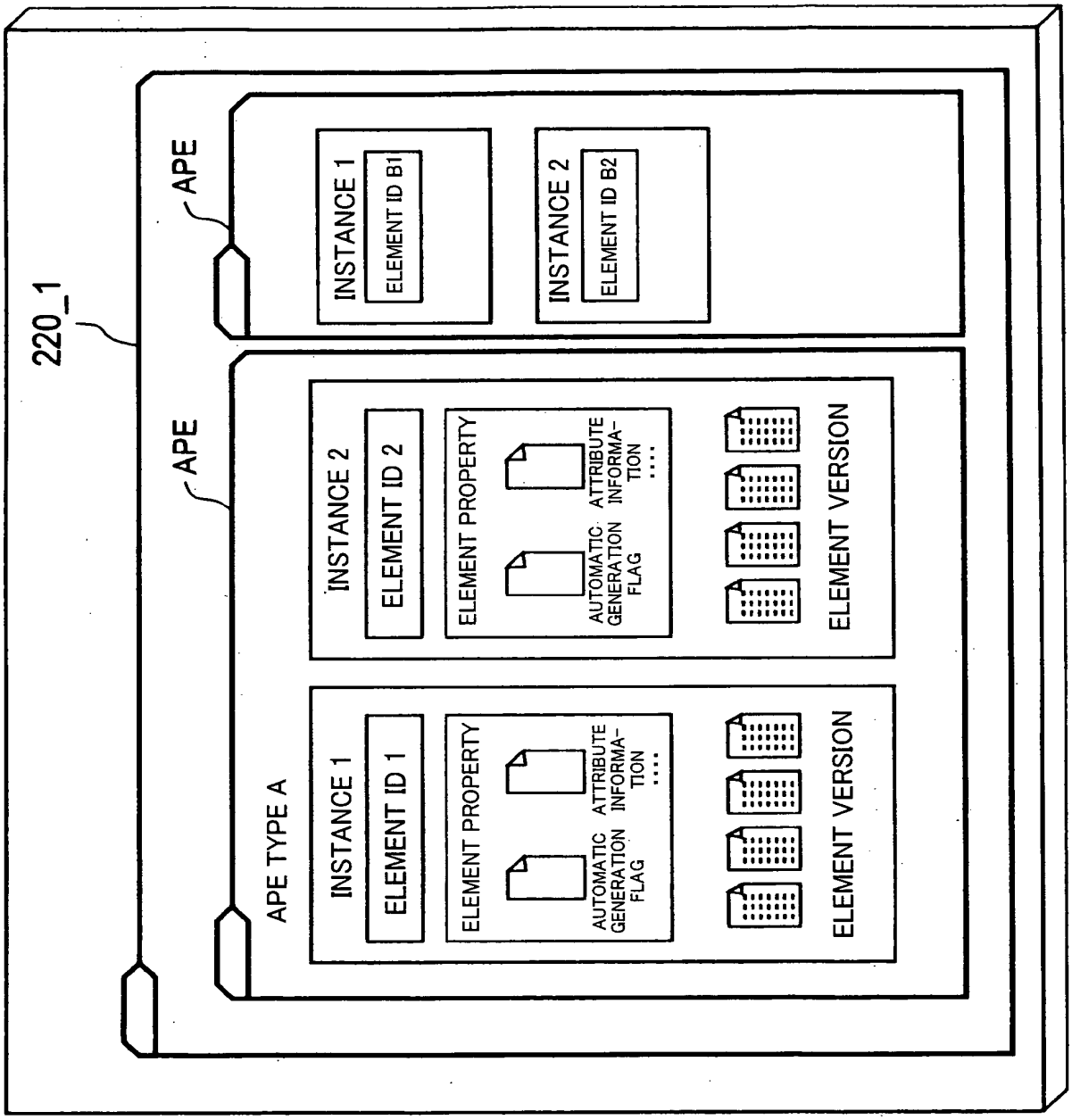

220_1
APE
APE TYPE A
INSTANCE 1
ELEMENT ID 1
ELEMENT PROPERTY
AUTOMATIC GENERATION FLAG
ATTRIBUTE INFORMATION
ELEMENT VERSION
INSTANCE 2
ELEMENT ID 2
ELEMENT PROPERTY
AUTOMATIC GENERATION FLAG
ATTRIBUTE INFORMATION
ELEMENT VERSION
APE
INSTANCE 1
ELEMENT ID B1
INSTANCE 2
ELEMENT ID B2

FIG. 15

APE TYPE NUMBER	APE TYPE
...	IC SYSTEM KEY
...	IC AREA KEY
...	IC SERVICE KEY
...	IC SYNTHETIC KEY
...	IC KEY CHANGE PACKAGE
...	IC ISSUANCE KEY PACKAGE
...	IC EXPANSION ISSUANCE KEY PACKAGE
...	IC AREA REGISTRATION KEY PACKAGE
...	IC AREA DELETION KEY PACKAGE
...	IC SERVICE REGISTRATION KEY PACKAGE
...	IC SERVICE DELETION KEY PACKAGE
...	IC MEMORY DIVISION KEY PACKAGE
...	IC MEMORY DIVISION ELEMENT KEY PACKAGE
...	OBSTACLE RECORDING FILE
...	MUTUAL AUTHENTICATION USE KEY
...	PACKAGE KEY
...	NEGATIVE LIST
...	SERVICE DATA TEMPORARY FILE

FIG. 16

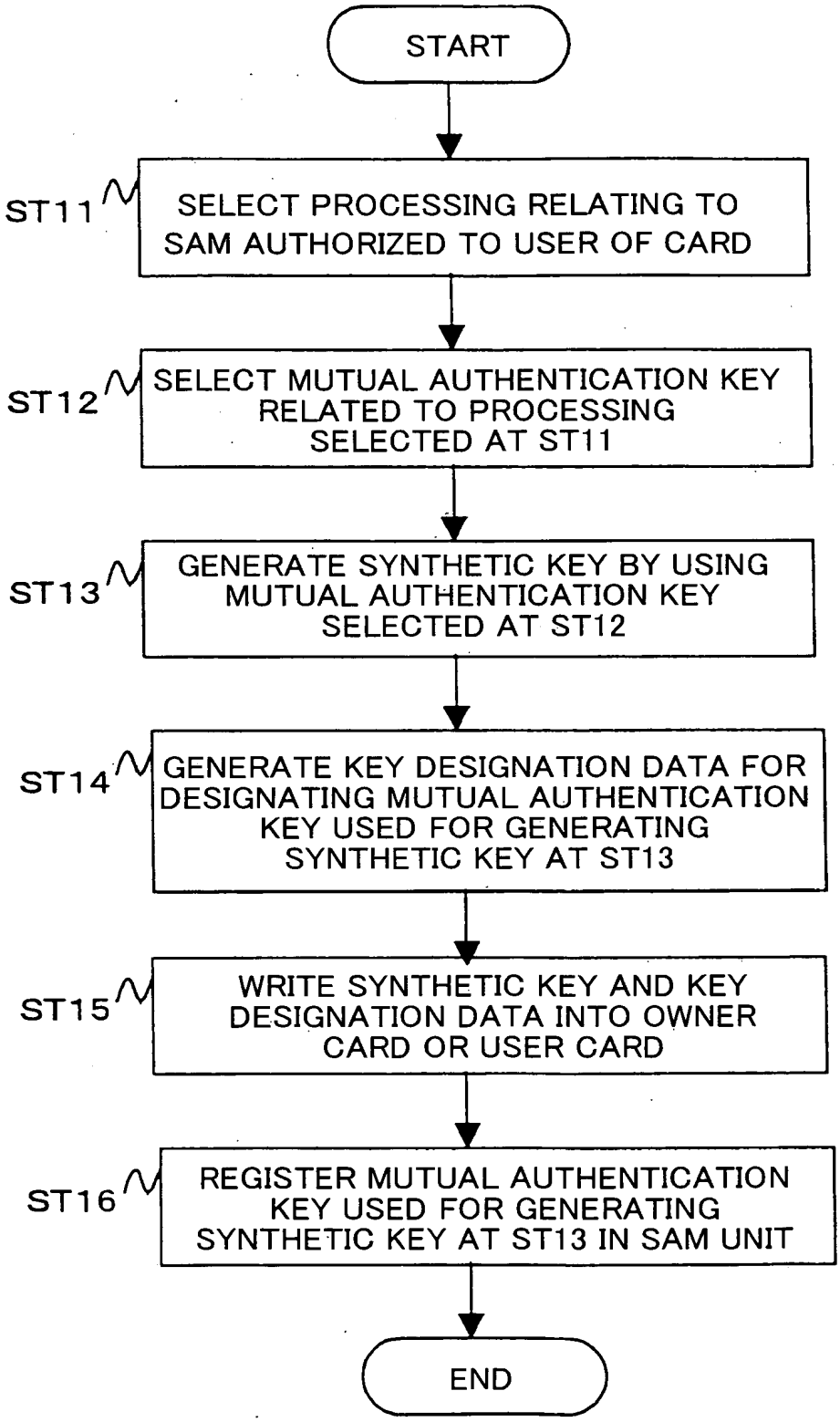

START
ST11
SELECT PROCESSING RELATING TO SAM AUTHORIZED TO USER OF CARD
ST12
SELECT MUTUAL AUTHENTICATION KEY RELATED TO PROCESSING SELECTED AT ST11
ST13
GENERATE SYNTHETIC KEY BY USING MUTUAL AUTHENTICATION KEY SELECTED AT ST12
ST14
GENERATE KEY DESIGNATION DATA FOR DESIGNATING MUTUAL AUTHENTICATION KEY USED FOR GENERATING SYNTHETIC KEY AT ST13
ST15
WRITE SYNTHETIC KEY AND KEY DESIGNATION DATA INTO OWNER CARD OR USER CARD
ST16
REGISTER MUTUAL AUTHENTICATION KEY USED FOR GENERATING SYNTHETIC KEY AT ST13 IN SAM UNIT
END

FIG. 17

MUTUAL AUTHENTICATION KEY NAME	AP MEMORY AREA -ID	APE TYPE NUMBER	INSTANCE NUMBER	ELEMENT VERSION
DEVICE KEY	...	...	...	...
TERMINATION KEY	...	...	...	...
MANUFACTURER SETTING SERVICE MUTUAL AUTHENTICATION KEY	...	...	...	...
HARDWARE MANAGEMENT SERVICE MUTUAL AUTHENTICATION KEY	...	...	...	...
COMMUNICATION MANAGEMENT SERVICE MUTUAL AUTHENTICATION KEY	...	...	...	...
MUTUAL AUTHENTICATION SERVICE MUTUAL AUTHENTICATION KEY	...	...	...	...
AP MEMORY AREA MANAGEMENT SERVICE MUTUAL AUTHENTICATION KEY	...	...	...	...
SERVICE AP MEMORY AREA MUTUAL AUTHENTICATION KEY	...	...	...	...
SYSTEM AP MEMORY AREA MUTUAL AUTHENTICATION KEY	...	...	...	...
MANUFACTURER AP MEMORY AREA MUTUAL AUTHENTICATION KEY	...	...	...	...

10/527651

FIG. 18

AP MEMORY AREA ID	ELEMENT TYPE NUMBER	ELEMENT INSTANCE NUMBER	ELEMENT VERSION NUMBER
2 BYTES	2 BYTES	2 BYTES	2 BYTES
AP RESOURCE AREA TO WHICH IT BELONGS	MUTUAL AUTHENTICATION KEY (FIXED VALUE)	ID OF RELEASE KEY RING	VERSION NUMBER OF USED KEY

FIG. 19A

MUTUAL AUTHENTICATION KEY NAME	AP MEMORY AREA·ID	APE TYPE NUMBER	INSTANCE NUMBER	ELEMENT VERSION
DEVICE KEY	•••	•••	•••	•••
HARDWARE MANAGEMENT SERVICE MUTUAL AUTHENTICATION KEY	•••	•••	•••	•••
COMMUNICATION MANAGEMENT SERVICE MUTUAL AUTHENTICATION KEY	•••	•••	•••	•••
AP MEMORY AREA MANAGEMENT SERVICE MUTUAL AUTHENTICATION KEY	•••	•••	•••	•••
SERVICE AP MEMORY AREA AP-R MUTUAL AUTHENTICATION KEY	•••	•••	•••	•••
TERMINATION KEY	•••	•••	•••	•••

FIG. 19B

• COMMAND WHICH CAN BE EXECUTED

SERVICE TYPE	COMMAND NAME
HARDWARE MANAGEMENT SERVICE	•••
COMMUNICATION MANAGEMENT SERVICE	•••
IC SERVICE	•••
MUTUAL AUTHENTICATION SERVICE	•••
AP MEMORY AREA MANAGEMENT SERVICE	•••

FIG. 20

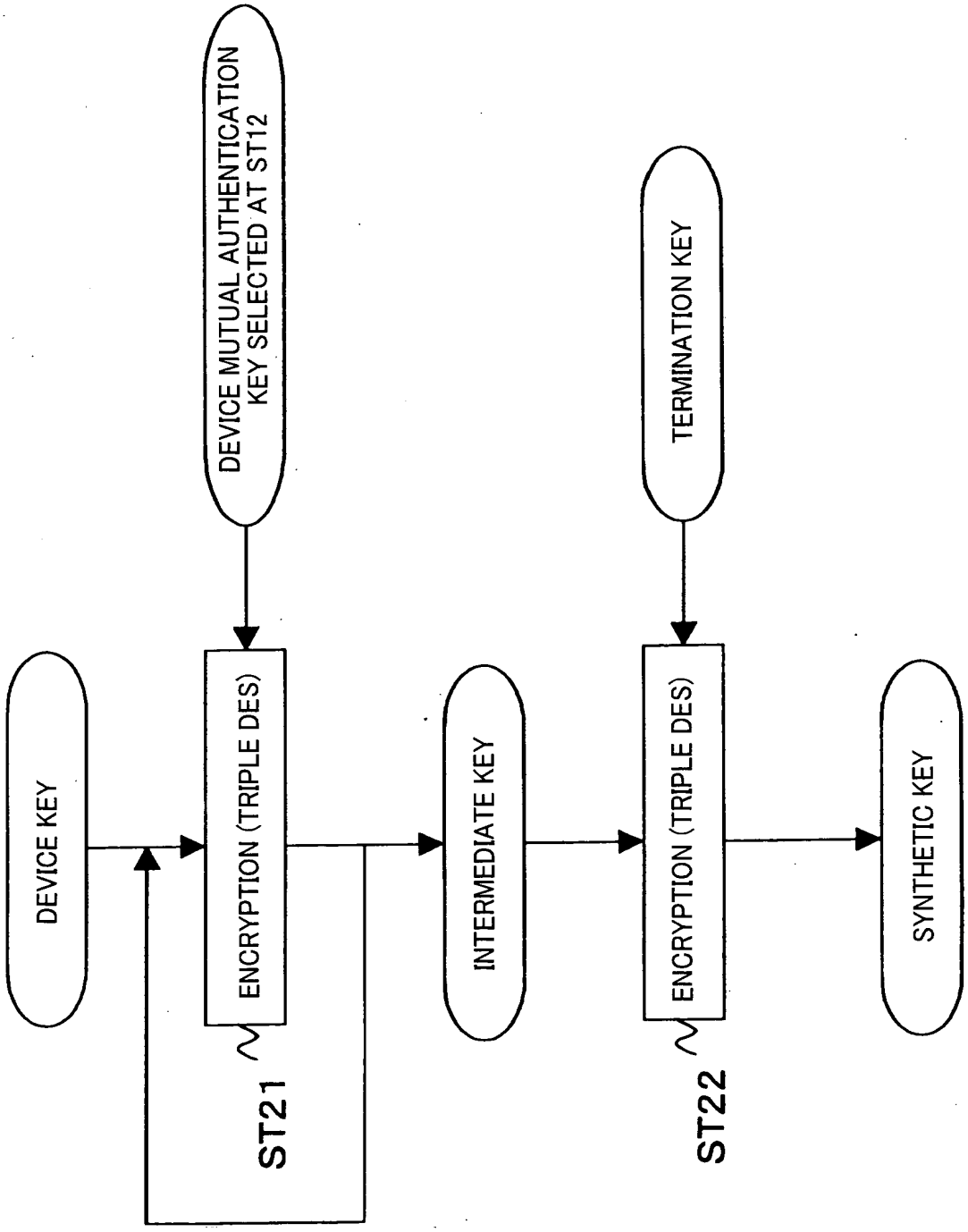

DEVICE MUTUAL AUTHENTICATION KEY SELECTED AT ST12
TERMINATION KEY
DEVICE KEY
ENCRYPTION (TRIPLE DES)
INTERMEDIATE KEY
ENCRYPTION (TRIPLE DES)
SYNTHETIC KEY
ST21
ST22

FIG. 21

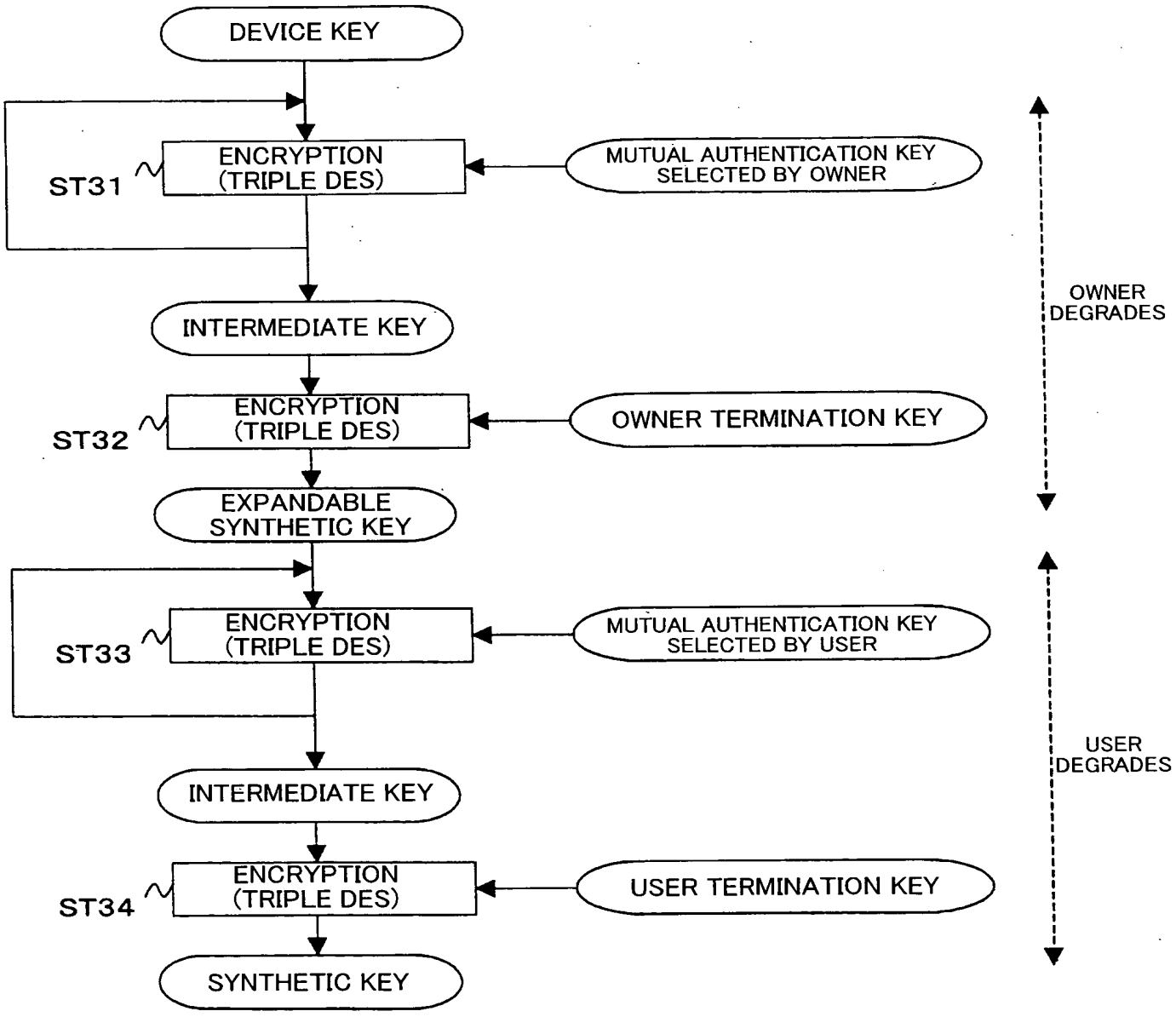

DEVICE KEY
ST31
ENCRYPTION (TRIPLE DES)
MUTUAL AUTHENTICATION KEY SELECTED BY OWNER
INTERMEDIATE KEY
ST32
ENCRYPTION (TRIPLE DES)
OWNER TERMINATION KEY
EXPANDABLE SYNTHETIC KEY
ST33
ENCRYPTION (TRIPLE DES)
MUTUAL AUTHENTICATION KEY SELECTED BY USER
INTERMEDIATE KEY
ST34
ENCRYPTION (TRIPLE DES)
USER TERMINATION KEY
SYNTHETIC KEY
OWNER DEGRADES
USER DEGRADES

FIG. 22

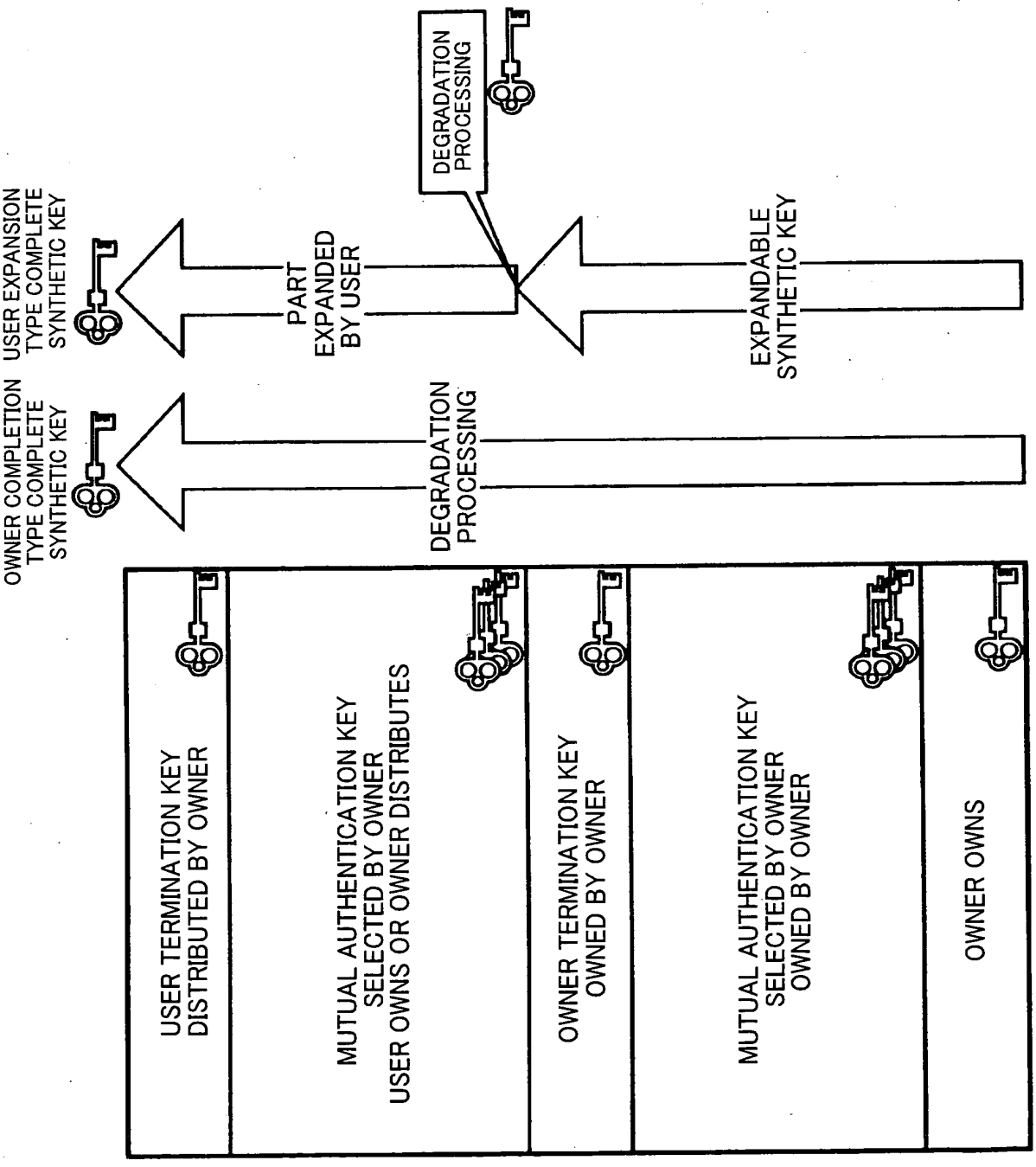

USER TERMINATION KEY
DISTRIBUTED BY OWNER
MUTUAL AUTHENTICATION KEY
SELECTED BY OWNER
USER OWNS OR OWNER DISTRIBUTES
OWNER TERMINATION KEY
OWNED BY OWNER
MUTUAL AUTHENTICATION KEY
SELECTED BY OWNER
OWNED BY OWNER
OWNER OWNS
DEGRADATION PROCESSING
OWNER COMPLETION TYPE COMPLETE SYNTHETIC KEY
DEGRADATION PROCESSING
EXPANDABLE SYNTHETIC KEY
PART EXPANDED BY USER
USER EXPANSION TYPE COMPLETE SYNTHETIC KEY

FIG. 23

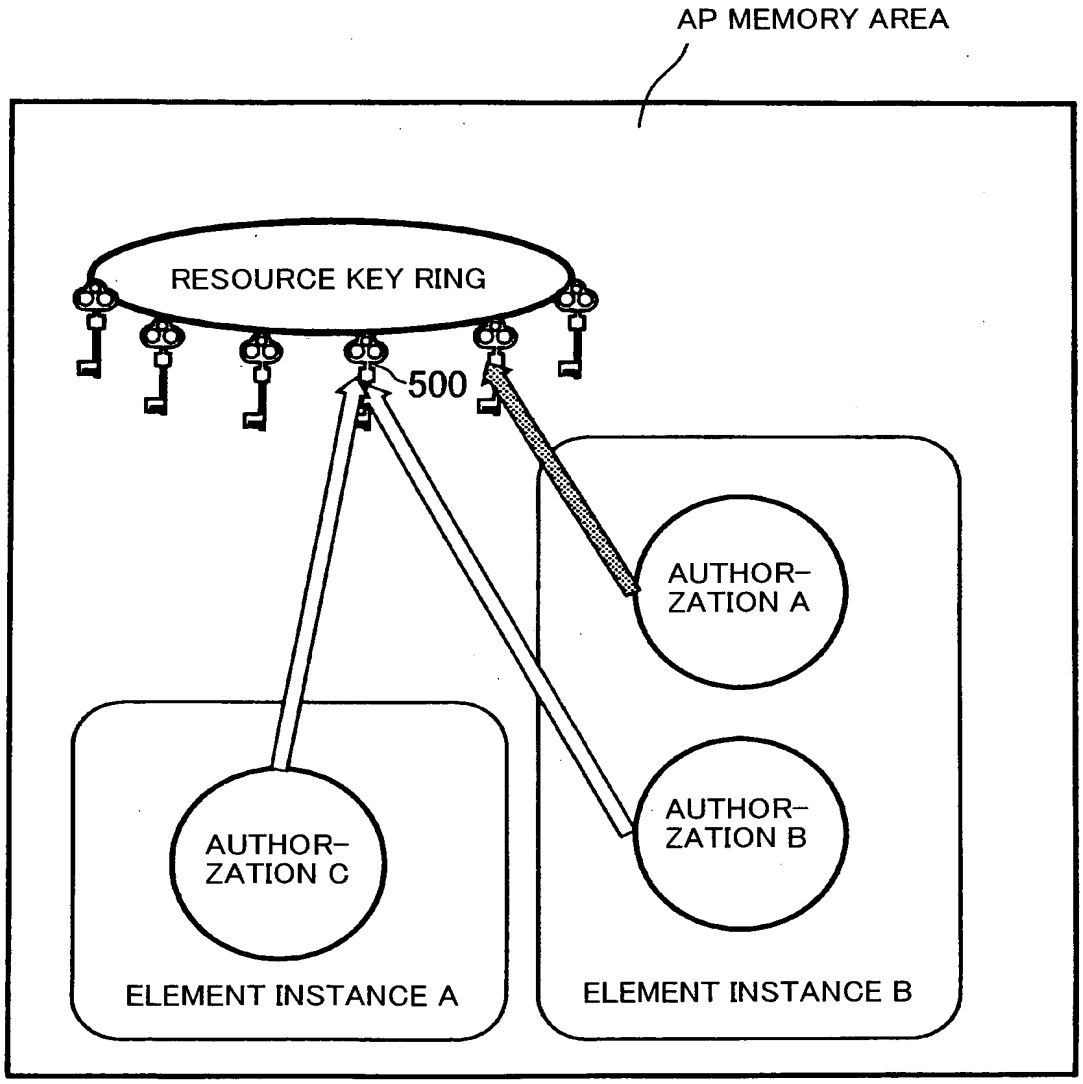

AP MEMORY AREA
RESOURCE KEY RING
500
AUTHOR-
ZATION A
AUTHOR-
ZATION B
AUTHOR-
ZATION C
ELEMENT INSTANCE A
ELEMENT INSTANCE B

FIG. 24

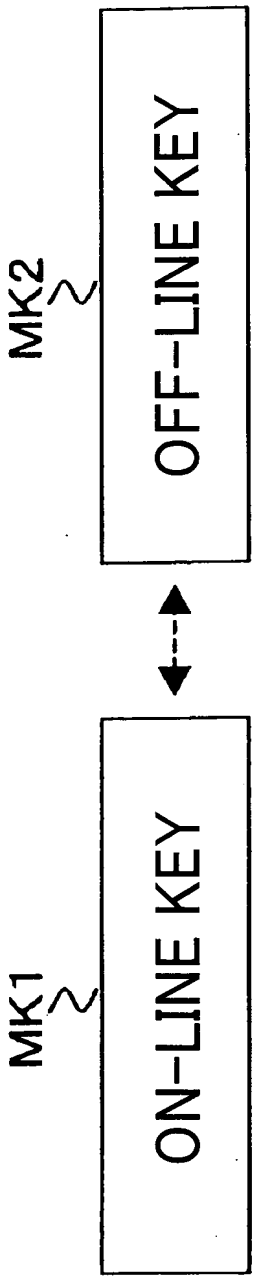


FIG. 25

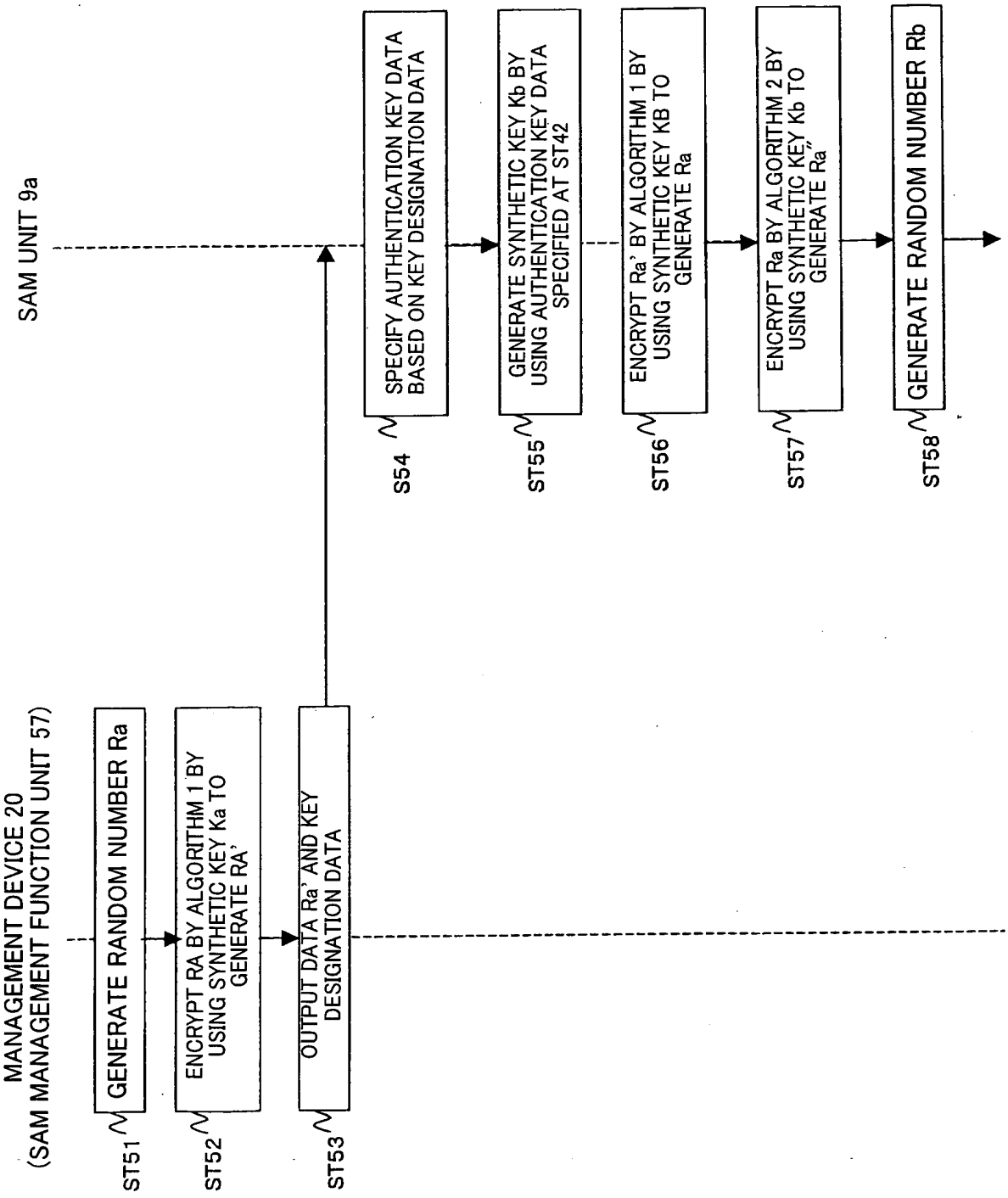

MANAGEMENT DEVICE 20
(SAM MANAGEMENT FUNCTION UNIT 57)
SAM UNIT 9a
GENERATE RANDOM NUMBER Ra
ST51
ENCRYPT RA BY ALGORITHM 1 BY USING SYNTHETIC KEY Ka TO GENERATE RA'
ST52
OUTPUT DATA Ra' AND KEY DESIGNATION DATA
ST53
SPECIFY AUTHENTICATION KEY DATA BASED ON KEY DESIGNATION DATA
S54
GENERATE SYNTHETIC KEY Kb BY USING AUTHENTICATION KEY DATA SPECIFIED AT ST42
ST55
ENCRYPT Ra' BY ALGORITHM 1 BY USING SYNTHETIC KEY KB TO GENERATE Ra
ST56
ENCRYPT Ra BY ALGORITHM 2 BY USING SYNTHETIC KEY Kb TO GENERATE Ra"
ST57
GENERATE RANDOM NUMBER Rb
ST58

FIG. 26

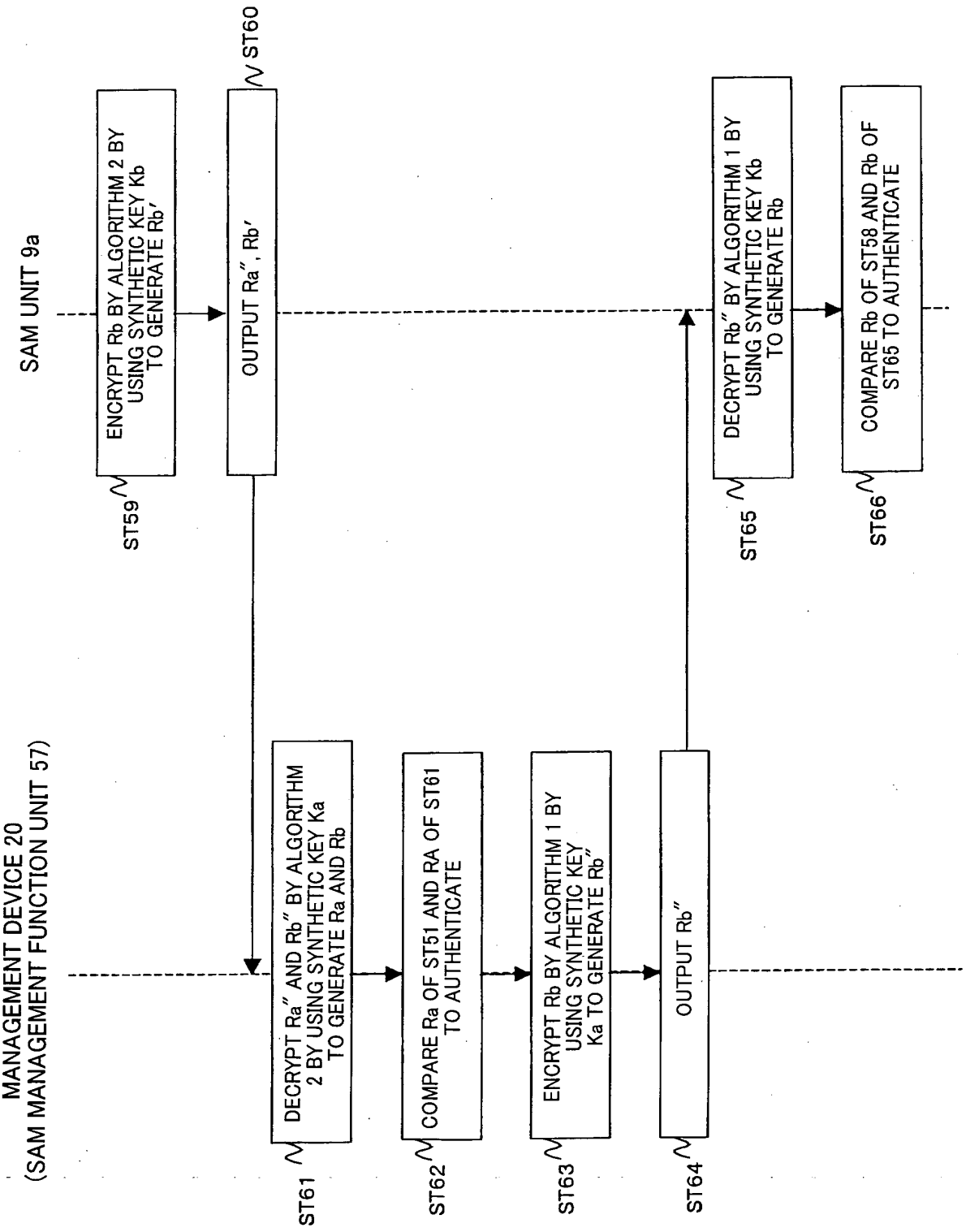
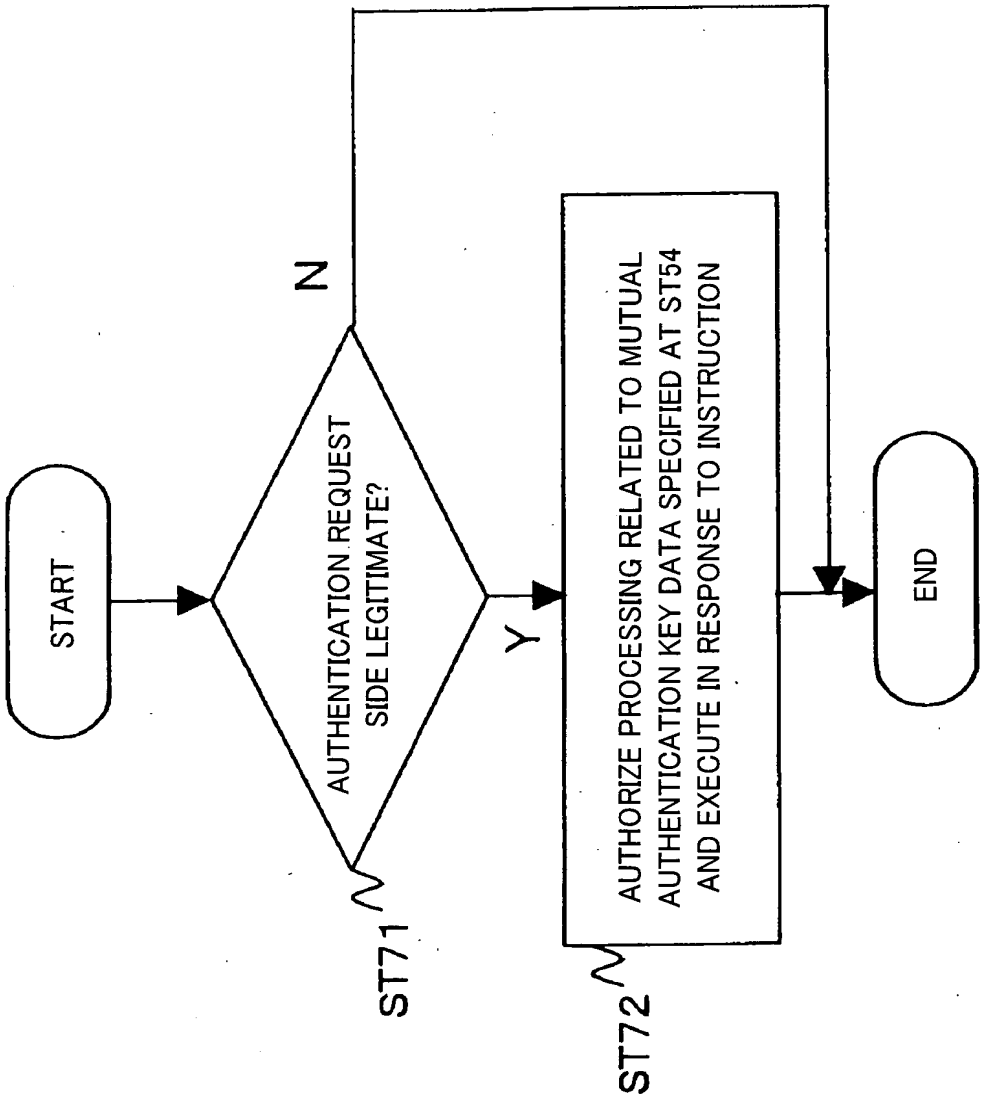

SAM UNIT 9a
MANAGEMENT DEVICE 20
(SAM MANAGEMENT FUNCTION UNIT 57)
ENCRYPT Rb BY ALGORITHM 2 BY USING SYNTHETIC KEY Kb TO GENERATE Rb'
ST59
OUTPUT Ra", Rb'
ST60
DECRYPT Ra" AND Rb" BY ALGORITHM 2 BY USING SYNTHETIC KEY Ka TO GENERATE Ra AND Rb
ST61
COMPARE Ra OF ST51 AND RA OF ST61 TO AUTHENTICATE
ST62
ENCRYPT Rb BY ALGORITHM 1 BY USING SYNTHETIC KEY Ka TO GENERATE Rb"
ST63
OUTPUT Rb"
ST64
DECRYPT Rb" BY ALGORITHM 1 BY USING SYNTHETIC KEY Kb TO GENERATE Rb
ST65
COMPARE Rb OF ST58 AND Rb OF ST65 TO AUTHENTICATE
ST66

FIG. 27


START
AUTHENTICATION REQUEST SIDE LEGITIMATE?
N
Y
ST71
AUTHORIZE PROCESSING RELATED TO MUTUAL AUTHENTICATION KEY DATA SPECIFIED AT ST54 AND EXECUTE IN RESPONSE TO INSTRUCTION
ST72
END

LIST OF REFERENCES

1... communication system

2... server apparatus

3... IC card

4... card RW

6... PC

7... external memory

8... SAM module

9a, 9b... SAM units

19a, 19b... ASP server apparatus

20... management device

51... AP edit tool

52... management tool

53... card reader/writer

54... display

55... I/F, 56... operating unit

57... SAM management function portion

58... card management function portion

61... memory I/F

62... external I/F

63... memory

64... authentication unit

65... CPU

71... default card

72... owner card

73... user card

74... transport card

75... AP encryption card

301... data processing system

302, 303... data processing device

310... memory

311... authentication unit

312... encryption unit

313... interface

314... CPU

330... memory

331... authentication unit

332... decryption unit

333... I/F